(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 281 059 A2**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **88103014.2**

(51) Int. Cl.4: **G07F 7/10** , H04L 9/02

(22) Anmeldetag: **29.02.88**

(30) Priorität: **04.03.87 DE 3706958**

(43) Veröffentlichungstag der Anmeldung: **07.09.88 Patentblatt 88/36**

(84) Benannte Vertragsstaaten: **AT BE CH DE ES FR GB IT LI NL SE**

(71) Anmelder: **Siemens Aktiengesellschaft Berlin und München**
Wittelsbacherplatz 2
D-8000 München 2(DE)

(72) Erfinder: **Kruse, Dietrich**
Ulmenstrasse 9
D-8012 Ottobrunn(DE)
Erfinder: **Beutelspacher, Albrecht, Prof.**
Schwalbenstrasse 78
D-8012 Ottobrunn(DE)
Erfinder: **Kersten, Annette-Gabrielle**
Frauenlobstrasse 6
D-6200 Wiesbaden(DE)

(54) Datenaustauschsystem mit mehreren jeweils eine Chipkarten-Leseeinrichtung enthaltenden Benutzerterminals.

(57) Ein für alle Benutzerterminals gleicher Geheimschlüssel (Ki) wird aus zwei Teilkomponenten (KTi, KT'i) gebildet, von denen die eine (KTi) in einem löschbaren programmierbaren Lesespeicher (EEPROM) hinterlegt ist. Für die zweite Teilkomponente (KT'i) wird ein verschlüsselter Datenblock (E(KT'i)) von außen an eine im Sicherheitsmodul vorgesehene Decodiereinrichtung (DEC) übertragen, deren entschlüsseltes Ausgangssignal als zweite Teilkomponente (KT'i) in einem ersten Teilbereich eines im Sicherheitsmodul des Benutzerterminals vorhandenen Schreib-Lese-Speichers (RAM) abgespeichert wird. Aus beiden Teilkomponenten (KTi, KT'i) wird ein Gesamtschlüssel (Ki) errechnet und das Ergebnis in einem zweiten Teilbereich des Schreib-Lese-Speichers (RAM) abgespeichert. ◆

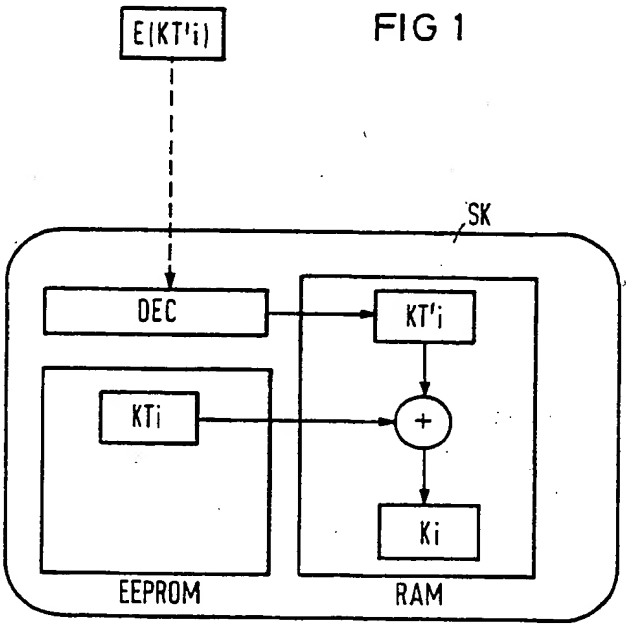


FIG 1

EP 0 281 059 A2

Datenaustauschsystem mit mehreren jeweils eine Chipkarten-Leseeinrichtung enthaltenden Benutzerterminals

Die Erfindung betrifft ein Datenaustauschsystem gemäß den Merkmalen des Oberbegriffs des Anspruchs 1.

In modernen Datenverarbeitungs-und Kommunikationssystemen spielt der Schutz der Daten eine immer wichtigere Rolle. Die Qualität eines Systems in bezug auf einen ausreichenden Datenschutz hängt dabei entscheidend davon ab, inwieweit es gelingt, daß der Zugriff zum System nur für berechtigte Personen möglich ist und umgekehrt nicht berechtigte Personen mit absoluter Sicherheit ausgesperrt bleiben. Eine einfache wenn auch nicht absolut sichere Möglichkeit zur Überprüfung der Zugriffsberechtigung zu einem System sind zum Beispiel sogenannte Paßwörter, die nur dem berechtigten Benutzer bekannt und die vom Benutzer beliebig oft geändert werden können. Da bei Paßwörtern die Gefahr besteht, daß sie von Unbefugten ausgespäht oder abgehört werden können, sind zusätzliche Sicherungsmaßnahmen unverzichtbar. Eine dieser Maßnahmen ist zum Beispiel die Ver-und Entschlüsselung der übertragenen Information, eine Maßnahme, die bei Datenverarbeitungssysemen unter anderem auch mit Hilfe der Chipkarte realisierbar ist. Mit der zunehmenden Einbeziehung der Chipkarte in Datenverarbeitungssysteme entsteht andererseits wieder ein zusätzliches Sicherheitsrisiko, weil Chipkarten relativ leicht verlorengehen können. Es muß deshalb unbedingt dafür gesorgt werden, daß die Chipkarte bei Verlust in jedem Fall vor einem eventuellen Mißbrauch geschützt ist. Die Chipkarte ist deshalb so konzipiert, daß auf die in einer gesicherten Chipkarte gespeicherten Daten nur dann zugegriffen werden kann, wenn vom Benutzer vorab ein nur in der Chipkarte abgespeicherter Identifikator, beispielsweise eine persönliche Identifikationsnummer, die soge nannte PIN, eingegeben wird.

Eine weitere Sicherheitsbarriere kann mit Hilfe der Authentifikation der Chipkarte zum System aufgebaut werden. Diese Authentifikation verhindert, daß ein beliebiger Teilnehmer durch die Vorgabe, befugt zu sein, an geheime Informationen im System gelangen kann. Eine wesentliche Voraussetzung für die Authentifikation ist ein persönliches, nicht kopierbares Merkmal des Teilnehmers. Dieses nichtkopierbare Merkmal des Teilnehmers wird mit Hilfe eines geheimen Schlüssels für die Ver-und Entschlüsselung erreicht, der den beiden Partnern, das heißt einerseits der Chipkarte und andererseits dem System, und zwar nur diesen beiden Partnern bekannt ist.

In einem POS-Banking-System auf Chipkartenbasis wird beispielsweise davon ausgegangen, daß geheime Daten im Kassenterminal in einem eigenen Sicherheitsmodul, zum Beispiel in einer sogenannten Sicherheitschipkarte gespeichert werden. Bei der Verwendung eines symmetrischen Verschlüsselungsalgorithmus muß in allen Terminals der gleiche geheime Terminalschlüssel existieren. Dieser Schlüssel wird benötigt, um aus der Kartenidentifizierungsnummer einer Kundenkarte einen gemeinsamen Kommunikationsschlüssel zu berechnen. Die Existenz eines universellen geheimen Schlüssels im Sicherheitsmodul bzw. in der Sicherheitschipkarte jedes POS-Terminals eines Gesamtsystems ist aber ein äußerst kritischer Punkt und gewissermaßen die Schwachstelle des Systems. Es sind deshalb bereits mehrere Schutzmaßnahmen überlegt worden, die das Bekanntwerden eines geheimen Globalschlüssels erschweren. Gemäß einer ersten Schutzmaßnahme gibt es anstelle eines einzigen geheimen Globalschlüssels K eine Serie von n verschiedenen Globalschlüsseln Kl, ..., Kn und dementsprechend unterschiedeliche Terminaltypen. Bei einem eventuellen Bekanntwerden eines dieser Schlüssel wird somit nicht das gesamte System gefährdet. Allerdings muß eine Kundenkarte auch n verschiedene Schlüssel KKl, ... KKn enthalten, von denen an einem bestimmten Terminal nur jeweils ein einziger gültig ist. Bei einer zweiten Schutz maßnahme sind ebenfalls mehrere Schlüssel Kl, ..., Kn vorgesehen, die n gewissen Zeitabständen zyklisch gewechselt werden. Auf diese Weise ergeben sich zum Beispiel mehrere Terminalschlüssel Klp, ..., Knp, die in der Zeitphase p gültig sind. In einer Kundenchipkarte müssen dann selbstverständlich auch die dazugehörigen Kundenschlüssel KKlp, ..., KKnp vorhanden sein.

Der vorliegenden Erfindung liegt nun die Aufgabe zugrunde, für die Sicherung eines globalen Geheimschlssels einen möglichst optimalen Lösungsweg zu finden, der die Ausforschung des jeweils gültigen Globalschlüssels praktisch unmöglich macht.

Die Lösung dieser Aufgabe ergibt sich erfindungsgemäß durch die kennzeichnenden Merkmale des Anspruchs 1. Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen angegeben. Durch die Aufsplittung des Geheimschlüssels in zwei Teilkomponenten, von denen eine Teilkomponente variabel ist, ergeben sich bei der regelmäßigen Neubildung entsprechend unterschiedliche neue Geheimschlüssel, so daß auch im Falle einer Ausforschung eines Schlüssels dieser

ausgeforschte Schlüssel sehr bald unaktuell und damit unbrauchbar sein wird.

Ein Ausführungsbeispiel der Erfindung wird im folgenden anhand der Zeichnung näher erläutert. Dabei zeigen

FIG 1 eine Schaltungsanordnung zur Generierung eines geheimen Globalschlüssels aus zwei Teilkomponenten

FIG 2 eine Variante zur Schaltung nach FIG 1 bezüglich einer Teilkomponente.

Die FIG 1 zeigt die für die Erläuterung der Erfindung wesentlichen Merkmale einer Sicherheitschipkarte SK in einem Benutzerterminal. Dem Ganzen liegt die Überlegung zugrunde, daß ein Globalschlüssel aus Sicherheitsgründen zunächst nicht komplett im Terminal gespeichert sein soll. Aus diesem Grund ist eine Aufsplittung des in der Sicherheitskarte hinterlegten geheimen Globalschlüssels Ki in zwei terinalspezifische Teilkomponenten KTi und KT'i vorgesehen. Die erste Teilkomponente KTi steht dabei geschützt in einem löschbaren programmierbaren Lesespeicher EEPROM, während die zweite Teilkomponente KT'i im Rahmen der täglichen Terminalanmeldungsprozedur in das Sicherheitsmodul des Terminals, das heißt in die Sicherheitskarte SK übertragen wird. Letzteres geschieht in der Weise, daß eine verschlüsselte zweite Teilkomponente E(KT'i) einer Decodierstufe DEC zugeführt wird, deren decodiertes Ausgangssignal als zweite Teilkomponente KT'i in einem ersten Teilbereich eines Schreib-Lese-Speichers RAM abgespeichert wird. Aus der im Lesespeicher EEPROM hinterlegten ersten Teilkomponente KTi und der in den Schreib-Lese-Speicher RAM übertragenen zweiten Teilkomponente KT'i wird schließlich der vollständige Geheimschlüssel Ki errechnet und das Ergebnis in einem zweiten Teilbereich des Schreib-Lese-Speichers RAM hinterlegt.

Die FIG 2 zeigt eine Variante zur Schaltung nach FiG 1 insofern, als die erste Teilkomponente KTi nicht a priori im Terminal verfügbar ist, sondern erst im Rahmen der Erstinbetriebnahme eines POS-Terminals generiert wird. Für diese Prozedur ist eine sogenannte Initialisierungschipkarte IK erforderlich. Arbeitet das Terminal zum Beispiel mit einer Sicherheitskarte SK, so wird in diese bei der Personalisierung ein Hilfsschlüssel Ko eingetragen. Mit Hilfe dieses Hilfsschlüssels Ko wird nun ein sogenannter Prä-Schlüssel KTi + Ko errechnet und in die Initialisierungschipkarte IK eingetragen. Nach gegenseitiger Authentifizierung zwischen der Sicherheitskarte SK und der Initialisierungschipkarte IK wird dieser Prä-Schlüssel KTi + Ko offen von der Initialisierungschipkarte IK an die Sicherheitskarte SK übergeben. Dort wird - schließlich aus dem Prä-Schlüssel KTi + Ko und dem bereits vorher hinterlegten Hilfsschlüssel Ko die erste Teilkomponente KTi berechnet und im Lesespeicher EEPROM der Sicherheitskarte SK eingetragen. Ob die auf diese Weise erfolgte Generierung der ersten Teilkomponente KTi des Globalschlüssels tatsächlich fehlerfrei abgelaufen ist, kann anschließend mit einer Testchipkarte überprüft werden.

Ansprüche

1. Datenaustauschsystem mit mehreren, jeweils eine Chipkarten-Leseeinrichtung enthaltenden Benutzerterminals, bei denen in einem Sicherheitsmodul ein für alle Benutzerterminals gleicher Geheimschlüssel hinterlegt ist, **dadurch gekennzeichnet,** daß der Geheimschlüssel (Ki) aus zwei Teilkomponenten (KTi, KT'i) gebildet ist, von denen die eine (KTi) in einem löschbaren programmierbaren Lesespeicher (EEPROM) hinterlegt ist, daß für die zweite Teilkomponete (KT'i) ein verschlüsselter Datenblock (E(KT'i)) von außen an eine im Sicherheitsmodul vorgesehene Decodiereinrichtung (DEC) übertragen wird, deren entschlüsseltes Ausgangssignal als zweite Teilkomponente (KT'i) in einem ersten Teilbereich eines im Sicherheitsmodul vorhandenen Schreib-Lese-Speichers (RAM) abgespeichert wird und daß die beiden Teilkomponenten (KTi, KT'i) miteinander verknüpft und das Ergebnis als Gesamtschlüssel (Ki) in einem zweiten Teilbereich des Schreib-Lese-Speichers (RAM) abgespeichert wird.

2. Datenaustauschsystem nach Anspruch 1, **dadurch gekennzeichnet,** daß zur Generierung der ersten Teilkomponente (KTi) zunächst ein Hilfsschlüssel (Ko) im Sicherheitsmodul abgespeichert wird, daß aus diesem Hilfsschlüssel (Ko) und der ersten Teilkomponente (KTi) ein Prä-Schlüssel (KTi + Ko) errechnet und in eine Initialisierungskarte (IK) eingetragen wird und daß nach gegenseitiger Authentifizierung zwischen dem Sicherheitsmodul und der Initialisierungskarte (IK) und nach Übertragung des Prä-Schlüssels in das Sicherheitsmodul aus dem Prä-Schlüssel (KTi + Ko) und dem Hilfsschlüssel (Ko) die erste Teilkomponente (KTi) errechnet und im löschbaren programmierbaren Lesespeicher (EEPROM) eingetragen wird.

3. Dastenaustauschsystem nach Anspruch 1 oder 2, **dadurch gekennzeichnet,** daß das Sicher heitsmodul als steckbare Sicherheitskarte (SK) ausgebildet ist.

FIG 1

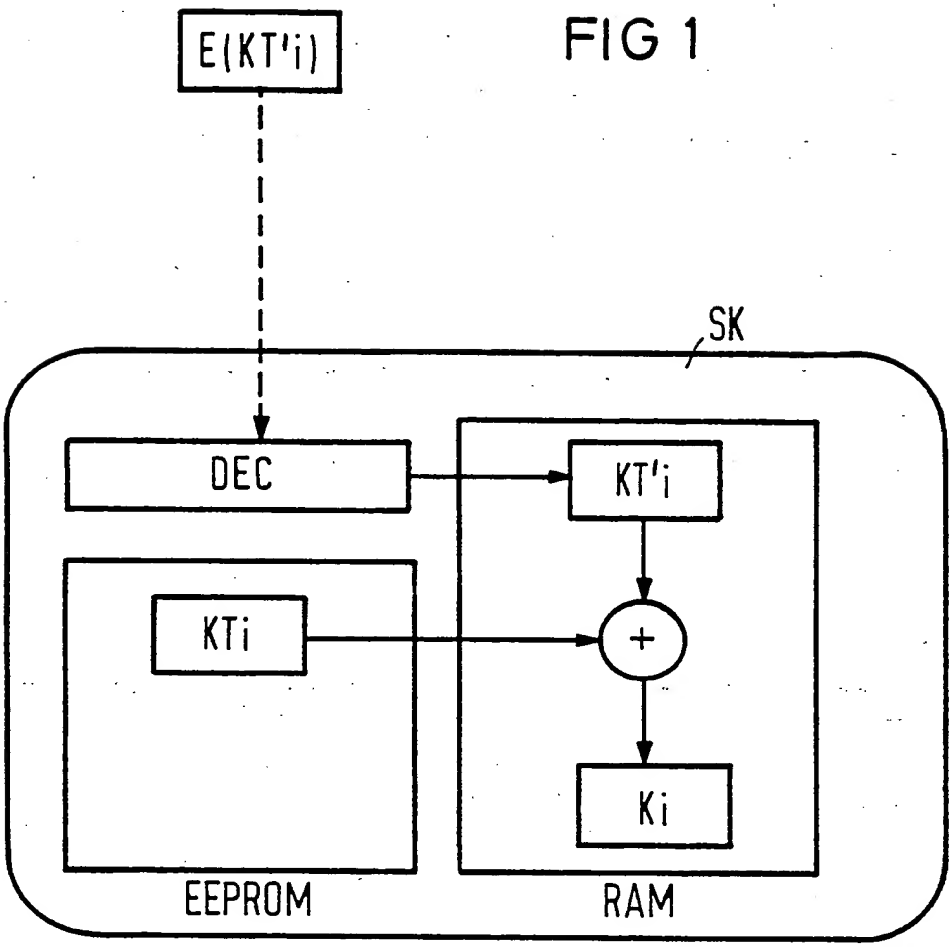
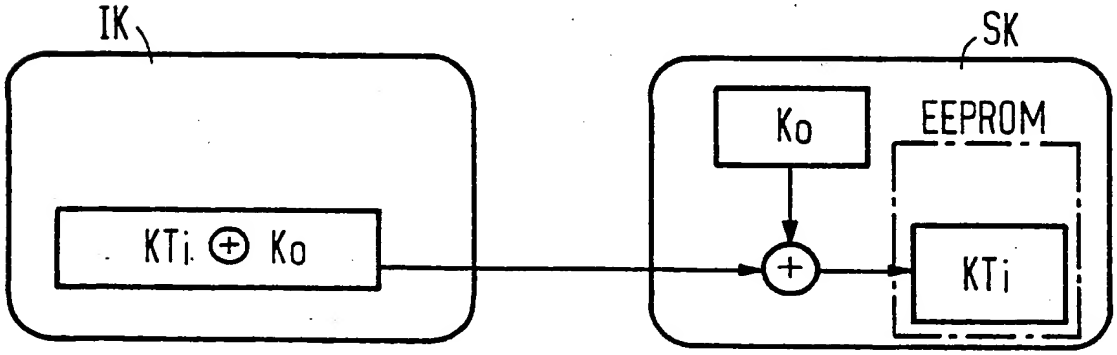


FIG 2



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 281 059**
A3

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: 88103014.2

(51) Int. Cl.5: **G07F 7/10 , H04L 9/02**

(22) Anmeldetag: **29.02.88**

(30) Priorität: **04.03.87 DE 3706958**

(43) Veröffentlichungstag der Anmeldung:
07.09.88 Patentblatt 88/36

(84) Benannte Vertragsstaaten:
AT BE CH DE ES FR GB IT LI NL SE

(88) Veröffentlichungstag des später veröffentlichten Recherchenberichts: **18.04.90 Patentblatt 90/16**

(71) Anmelder: **Siemens Aktiengesellschaft**
Wittelsbacherplatz 2
D-8000 München 2(DE)

(72) Erfinder: **Kruse, Dietrich**
Ulmenstrasse 9
D-8012 Ottobrunn(DE)
Erfinder: **Beutelspacher, Albrecht, Prof.**
Schwalbenstrasse 78
D-8012 Ottobrunn(DE)
Erfinder: **Kersten, Annette-Gabrielle**
Frauenlobstrasse 6
D-6200 Wiesbaden(DE)

(54) Datenaustauschsystem mit mehreren jeweils eine Chipkarten-Leseeinrichtung enthaltenden Benutzerterminals.

(57) Ein für alle Benutzerterminals gleicher Geheimschlüssel (Ki) wird aus zwei Teilkomponenten (KTi, KT'i) gebildet, von denen die eine (KTi) in einem löschbaren programmierbaren Lesespeicher (EEPROM) hinterlegt ist. Für die zweite Teilkomponente (KT'i) wird ein verschlüsselter Datenblock (E(KT'i)) von außen an eine im Sicherheitsmodul vorgesehene Decodiereinrichtung (DEC) übertragen, deren entschlüsseltes Ausgangssignal als zweite Teilkomponente (KT'i) in einem ersten Teilbereich eines im Sicherheitsmodul des Benutzerterminals vorhandenen Schreib-Lese-Speichers (RAM) abgespeichert wird. Aus beiden Teilkomponenten (KTi, KT'i) wird ein Gesamtschlüssel (Ki) errechnet und das Ergebnis in einem zweiten Teilbereich des Schreib-Lese-Speichers (RAM) abgespeichert.

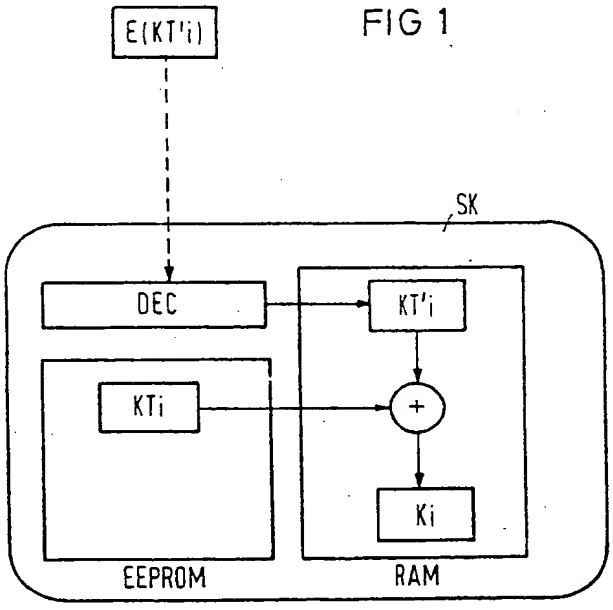


FIG 1

EP 0 281 059 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 88 10 3014

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.4)
A	EP-A-0140388 (ATALLA CORPORATION) * das ganze Dokument * ---	1-3	G07F7/10 H04L9/02
A	EP-A-0063794 (SIEMENS AKTIENGESELLSCHAFT) * Zusammenfassung; Ansprüche 1-8; Figuren 1-6 * ---	1-3	
A	EP-A-0198384 (SIEMENS AKTIENGESELLSCHAFT) * Zusammenfassung; Ansprüche 1-8; Figuren 1, 2 * * Spalte 1-4 * ---	1-3	
A	EP-A-0166541 (K. K. TOSHIBA) -----		

RECHERCHIERTE SACHGEBIETE (Int. Cl.4)
G07F H04L G06F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	20 FEBRUAR 1990	GUIVOL O.

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P0403)